STATE OF ALABAMA

Information Technology Standard

Standard 640-02S3: Dial-In Access/Modem Use

1. INTRODUCTION:

Dial-in access poses a considerable number of risks. A modem connection can bypass access controls the firewall provides, and expose the network to vulnerabilities the firewall was designed to protect against. Employees granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the State are literal extensions of the State network and that they provide a potential path to the State's most sensitive information.

2. OBJECTIVE:

Protect the State's electronic information resources from inadvertent compromise by authorized personnel using a dial-in connection by highlighting the risks associated with modem access, prohibiting modem use except where absolutely necessary, and ensuring required modems have been configured securely and are monitored effectively.

3. SCOPE:

These requirements apply to all authorized dial-in access users (State employees, contractors, vendors, and business partners) of any State of Alabama information system resources.

4. REQUIREMENTS:

4.1 DIAL-IN ACCESS

State employees and authorized third parties (customers, vendors, etc.) may, with the IT Manager's written approval, use dial-in connections to gain access to the State network.

Dial-in accounts are considered "as needed" accounts. If a dial-in account is not used for a period of six months the account shall be disabled. If dial-in access is subsequently required, the individual must request a new account.

Dialing directly into or out of a system that is simultaneously connected to the State's network infrastructure is prohibited, except as required for remote maintenance. Remote maintenance connections must comply with applicable State standards.

Dial-in access requires strong authentication consistent with authentication policy and remote access requirements.

It is the responsibility of employees with dial-in access privileges to ensure dial-in connections are not used by non-employees to gain access to State information system resources.

Account activity shall be monitored and audited to ensure that malicious activity is not occurring.

4.2 MODEM USE

The use of modems is generally prohibited except as described in this and other applicable standards.

Modems shall not be part of the standard desktop computer hardware configuration.

Modems shall not utilize auto-answer mode such that they are able to receive incoming dial-up calls.

4.3 EXCEPTIONS

Agencies requesting exception to these requirements shall include in security plans a migration plan addressing modem alternatives and stating when compliance will be attained.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Information Technology Policy 620-03: Authentication

Information Technology Standard 640-02S4: Remote Maintenance

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/16/2007	